

1 **KAZEROUNI LAW GROUP, APC**  
2 Abbas Kazerounian, Esq. (SBN 249203)  
3 ak@kazlg.com  
4 Mona Amini (SBN 296829)  
5 mona@kazlg.com  
6 245 Fischer Avenue, Unit D1  
7 Costa Mesa, California 92626  
8 Telephone: (800) 400-6808  
9 Facsimile: (800) 520-5523

10 *Attorneys for Plaintiff*  
11 Haris Mirza  
12  
13

14 **UNITED STATES DISTRICT COURT**  
15 **NORTHERN DISTRICT OF CALIFORNIA**

16 HARIS MIRZA, individually and on  
17 behalf of all others similarly situated,

18 Plaintiff,

19 vs.  
20 23ANDME, INC.,

21 Defendant.

22 Case No.: 3:23-cv-05259-JSC

23 CLASS ACTION COMPLAINT FOR  
24 VIOLATIONS OF:

1. CALIFORNIA CONSUMER  
2. PRIVACY ACT OF 2018, CAL. CIV.  
3. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR  
3. COMPETITION LAW, CAL. BUS.  
4. & PROF. CODE §§ 17200, *et. seq.*;
3. BREACH OF CONTRACT; and
4. NEGLIGENCE

25 JURY TRIAL DEMANDED

26 //

27 //

28 //

//

//

//

//

1 Plaintiff HARIS MIRZA (“Plaintiff”), individually and on behalf of the general  
 2 public and all others similarly situated (the “Class members”), by and through their  
 3 attorneys, upon personal knowledge as to facts pertaining to themselves and on  
 4 information and belief as to all other matters, brings this class action against Defendant  
 5 23ANDME, INC. (“Defendant” or “23andMe”) and alleges as follows:

6 **NATURE OF THE CASE**

7 1. This is a data breach class action arising out of Defendant’s failure to  
 8 implement and maintain reasonable security practices to protect consumers’ sensitive  
 9 personal information. For its business purposes, Defendant stores and transmits  
 10 personally identifiable information (“PII”) from customers including, but not limited  
 11 to, name, sex, date of birth, DNA and genetic ancestry results, profile photos,  
 12 geographical information, and other sensitive personal information.

13 2. On or about October 6, 2023, Defendant publicly announced via its  
 14 website<sup>1</sup> that customer profile information shared through its DNA Relatives feature<sup>2</sup>  
 15 was compiled from individual 23andMe.com accounts, without account users’  
 16 authorization, that contained the personally identifiable information (“PII”) and/or  
 17 protected health information (“PHI”) of its customers (the “Data Breach”).  
 18 Defendant’s website notice entitled “Addressing Data Security Concerns” further  
 19 stated, “[w]e believe that the threat actor may have then, in violation of  
 20 [Defendant’s] Terms of Service, accessed 23andMe.com accounts without  
 21 authorization and obtained information from certain accounts, including information  
 22 about users’ DNA Relatives profiles.”

23 3. On or about October 11, 2023, Defendant sent Plaintiff and similarly  
 24 situated Class members additional notifications via email related to the Data Breach,

---

26 <sup>1</sup> <https://blog.23andme.com/articles/addressing-data-security-concerns> (last accessed October 13,  
 27 2023)

28 <sup>2</sup> Through Defendant’s DNA Relatives feature available to the company’s 14 million users, any  
 account can search for others who may be even a distant genetic match, thus a single account can  
 see the accounts of thousands of other individuals who have information stored or maintained on  
 Defendant’s system or network.

1 which similarly stated, “[w]e recently learned that certain profile information – which  
 2 a customer creates and chooses to share with their genetic relatives in the DNA  
 3 Relatives feature – was accessed from individual 23andMe.com accounts. This was  
 4 done without the account users’ authorization.”

5       4.      Defendant’s Data Breach notifications were misleading and inadequate  
 6 and did not provide any detail regarding when or for how long the Data Breach  
 7 occurred. Further, Defendant’s Data Breach notices failed to indicate the scope of the  
 8 Data Breach or the specific information that was accessed, obtained from Defendant’s  
 9 system without authorization and whether any of the PII and/or PHI accessed and/or  
 10 exfiltrated by the unauthorized person was recovered.

11       5.      Defendant owed a duty to Plaintiff and Class members to implement and  
 12 maintain reasonable and adequate security measures to secure, protect, and safeguard  
 13 the PII and/or PHI it collected from consumers for business purposes and stored on its  
 14 systems or networks. This included ensuring information would not be shared with  
 15 unauthorized parties and that any third-party providers had security procedures in place  
 16 to maintain the security and integrity of any data to which Defendant gave them access  
 17 and sufficiently prevented unauthorized access to Defendant’s systems.

18       6.      Defendant breached its duty by, *inter alia*, failing to implement and  
 19 maintain reasonable security procedures and practices to protect PII and/or PHI from  
 20 unauthorized access and storing and retaining Plaintiff’s and Class members’ personal  
 21 information on inadequately protected systems.

22       7.      The Data Breach happened because of Defendant’s inadequate  
 23 cybersecurity, which caused Plaintiff’s and Class members’ PII and/or PHI to be  
 24 accessed, exfiltrated, and disclosed to unauthorized third parties in the Data Breach.  
 25 This action seeks to address and remedy these failings as Plaintiff brings this action on  
 26 behalf of himself and all affected individuals.



8. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for himself and the Class members, injunctive relief, including public injunctive relief, and actual damages.

## **JURISDICTION AND VENUE**

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

10. This Court has personal jurisdiction over Defendant because Defendant maintains a principal place of business within this District in South San Francisco, California and regularly conducts business in the State of California and within this District.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in and/or emanated from within this District.

## PARTIES

12. Plaintiff is a resident of Porter Ranch, California, and a citizen of the State of California. Upon information and belief, Plaintiff is a victim of the Data Breach and Plaintiff's information was among the data accessed and/or exfiltrated by an unauthorized third party in the Data Breach,

13. Sometime prior to October 6, 2023, Defendant received or obtained Plaintiff's personal information and/or Plaintiff provided their personal information to Defendant with the expectation that this information would be kept secure and not disclosed to, or permitted to be accessed by, unauthorized parties.

14. On or around October 11, 2023, Defendant sent Plaintiff an email with the subject “Update to our customers.” The email informed Plaintiff and other similarly situated Class members of the Data Breach.

1       15. After learning of the Data Breach, Plaintiff spent significant time and  
2 effort taking actions to attempt to mitigate the impact of the Data Breach, including  
3 monitoring accounts. This is time Plaintiff otherwise would have spent performing  
4 other activities or leisurely events for the enjoyment of life and this loss of time was a  
5 direct result of the Data Breach.

6       16. As a result of the Data Breach, Plaintiff has suffered invasion of privacy  
7 and emotional distress as a result of the unauthorized access and disclosure of their PII  
8 and/or PHI, which Defendant had a duty to protect from unauthorized disclosure,  
9 including anxiety, concern, and uneasiness about unauthorized parties having, viewing,  
10 and potentially using their personal information, including DNA information, as well  
11 as unease about Defendant having additional data breaches or otherwise disclosing  
12 their personal information in the future. In addition to Plaintiff suffering actual injury  
13 from lost time and invasion of privacy, Plaintiff also suffers the imminent and  
14 continuing injury arising from the heightened risk of fraud and identity theft due to the  
15 Data Breach. Upon information and belief, Plaintiff's and the Class members' personal  
16 information stolen from Defendant is already leaked and made available for sale and/or  
17 purchased by criminals on the dark web.<sup>3</sup>

18       17. As a result of Defendant's failure to implement and maintain reasonable  
19 security procedures and practices appropriate to the nature of the personal information  
20 it collected and maintained, Plaintiff's PII and/or PHI was accessed, exfiltrated, and  
21 otherwise disclosed to unauthorized third parties in the Data Breach.

22       18. Defendant is a corporation formed under the laws of the State of Delaware  
23 with a principal place of business located at 349 Oyster Point Blvd, South San  
24 Francisco, California.

25       19. The agents, servants and/or employees of the Defendant and each of them  
26 acting on behalf of the Defendant acted within the course and scope of his, her or its

---

27  
28       <sup>3</sup> <https://www.reuters.com/technology/hackers-advertise-sale-23andme-data-leaked-data-forum-2023-10-06/> (last accessed October 13, 2023)

1 authority as the agent, servant and/or employee of the Defendant, and personally  
 2 participated in the conduct alleged herein on behalf of the Defendant with respect to  
 3 the conduct alleged herein.

4 **FACTUAL ALLEGATIONS**

5 ***PII Is a Valuable Property Right that Must Be Protected***

6 20. The California Constitution guarantees every Californian a right to  
 7 privacy. And PII is a recognized valuable property right.<sup>4</sup> California has repeatedly  
 8 recognized this property right, most recently with the passage of the California  
 9 Consumer Privacy Act of 2018.

10 21. In a Federal Trade Commission (“FTC”) roundtable presentation, former  
 11 Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII  
 12 by observing:

13       Most consumers cannot begin to comprehend the types and  
 14 amount of information collected by businesses, or why their  
 15 information may be commercially valuable. Data is currency.  
 16 The larger the data set, the greater potential for analysis – and  
 17 profit.<sup>5</sup>

18 22. The value of PII as a commodity is measurable. “PII, which companies  
 19 obtain at little cost, has quantifiable value that is rapidly reaching a level comparable  
 20 to the value of traditional financial assets.”<sup>6</sup> It is so valuable to identity thieves that  
 21 once PII has been disclosed, criminals often trade it on the “cyber black-market” for  
 22 several years.

23 23. Companies recognize PII as an extremely valuable commodity akin to a  
 24 form of personal property. For example, Symantec Corporation’s Norton brand has  
 25 created a software application that values a person’s identity on the black market.<sup>7</sup>

---

26 24 <sup>4</sup> See John T. Soma, et al., *Corporate Privacy Trend: The “Value” of Personally Identifiable*  
 27 *Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at \*2  
 28 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a  
 29 level comparable to the value of traditional financial assets.”) (citations omitted).

25 25 <sup>5</sup> FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring  
 26 Privacy Roundtable) (Dec. 7, 2009), <https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable>.

27 27 <sup>6</sup> See Soma, *Corporate Privacy Trend*, *supra*.

28 28 <sup>7</sup> Risk Assessment Tool, Norton 2010, [www.everyclickmatters.com/victim/assessment-tool.html](http://www.everyclickmatters.com/victim/assessment-tool.html).

1       24. As a result of its real value and the recent large-scale data breaches,  
 2 identity thieves and cyber criminals openly post credit card numbers, Social Security  
 3 numbers, PII and other sensitive information directly on various illicit Internet websites  
 4 making the information publicly available for other criminals to take and use. This  
 5 information from various breaches, including the information exposed in the Data  
 6 Breach, can be aggregated and become more valuable to thieves and more damaging  
 7 to victims. In one study, researchers found hundreds of websites displaying stolen PII  
 8 and other sensitive information. Strikingly, none of these websites were blocked by  
 9 Google's safeguard filtering mechanism – the “Safe Browsing list.”

10      25. Recognizing the high value that consumers place on their PII, some  
 11 companies now offer consumers an opportunity to sell this information to advertisers  
 12 and other third parties. The idea is to give consumers more power and control over the  
 13 type of information they share – and who ultimately receives that information. By  
 14 making the transaction transparent, consumers will make a profit from the surrender of  
 15 their PII.<sup>8</sup> This business has created a new market for the sale and purchase of this  
 16 valuable data.<sup>9</sup>

17      26. Consumers place a high value not only on their PII, but also on the privacy  
 18 of that data. Researchers shed light on how much consumers value their data privacy –  
 19 and the amount is considerable. Indeed, studies confirm that “when privacy information  
 20 is made more salient and accessible, some consumers are willing to pay a premium to  
 21 purchase from privacy protective websites.”<sup>10</sup>

22  
 23  
 24  
 25      <sup>8</sup> Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010)  
 26      available at <https://www.nytimes.com/2010/07/18/business/18unboxed.html>.

27      <sup>9</sup>See Julia Angwin and Emil Steel, *Web’s Hot New Commodity: Privacy*, Wall Street Journal (Feb.  
 28, 2011) available at <https://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

28      <sup>10</sup>Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An  
 29      Experimental Study* Information Systems Research 22(2) 254, 254 (June 2011), available at  
[https://www.jstor.org/stable/23015560?seq=1#page\\_scan\\_tab\\_contents](https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents).

1       27. One study on website privacy determined that U.S. consumers valued the  
 2 restriction of improper access to their PII between \$11.33 and \$16.58 per website.<sup>11</sup>

3       28. Given these facts, any company that transacts business with a consumer  
 4 and then compromises the privacy of consumers' PII has thus deprived that consumer  
 5 of the full monetary value of the consumer's transaction with the company.

6       ***Theft of PII Has Grave and Lasting Consequences for Victims***

7       29. A data breach is an incident in which sensitive, protected, or confidential  
 8 data has potentially been viewed, stolen, or used by an individual unauthorized to do  
 9 so. As more consumers rely on the internet and apps on their phone and other devices  
 10 to conduct every-day transactions, data breaches are becoming increasingly more  
 11 harmful.

12       30. Theft or breach of PII is serious. The California Attorney General  
 13 recognizes that “[f]oundational” to every Californian’s constitutional right to privacy  
 14 is “information security: if companies collect consumers’ personal data, they have a  
 15 duty to secure it. An organization cannot protect people’s privacy without being able  
 16 to secure their data from unauthorized access.”<sup>12</sup>

17       31. The United States Government Accountability Office noted in a June 2007  
 18 report on Data Breaches (“GAO Report”) that identity thieves use PII to take over  
 19 existing financial accounts, open new financial accounts, receive government benefits  
 20 and incur charges and credit in a person’s name.<sup>13</sup> As the GAO Report states, this type  
 21 of identity theft is so harmful because it may take time for the victim to become aware  
 22 of the theft and can adversely impact the victim’s credit rating.

23       32. In addition, the GAO Report states that victims of identity theft will face  
 24 “substantial costs and inconveniences repairing damage to their credit records ... [and

---

26  
 27       <sup>11</sup>II-Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar.  
 28       2003) at table 3, available at <https://ideas.repec.org/p/wpa/wupio/0304001.html> (emphasis added).

27       <sup>12</sup>California Data Breach Report, Kamala D. Harris, Attorney General, California Department of  
 28       Justice, February 2016.

27       <sup>13</sup>See GAO, GAO Report 9 (2007) available at <http://www.gao.gov/new.items/d07737.pdf>.

1 their] good name.” According to the FTC, identity theft victims must spend countless  
 2 hours and large amounts of money repairing the impact to their good name and credit  
 3 record.<sup>14</sup>

4       33. Identity thieves use personal information for a variety of crimes, including  
 5 credit card fraud, phone or utilities fraud, and bank/finance fraud.<sup>15</sup> According to  
 6 Experian, “[t]he research shows that personal information is valuable to identity  
 7 thieves, and if they can get access to it, they will use it” to among other things: open a  
 8 new credit card or loan; change a billing address so the victim no longer receives bills;  
 9 open new utilities; obtain a mobile phone; open a bank account and write bad checks;  
 10 use a debit card number to withdraw funds; obtain a new driver’s license or ID; use the  
 11 victim’s information in the event of arrest or court action.<sup>16</sup>

12       34. According to the IBM and Ponemon Institute’s 2019 “Cost of a Data  
 13 Breach” report, the average cost of a data breach per consumer was \$150 per record.<sup>17</sup>  
 14 Other estimates have placed the costs even higher. The 2013 Norton Report estimated  
 15 that the average cost per victim of identity theft – a common result of data breaches –  
 16 was \$298 dollars.<sup>18</sup> And in 2019, Javelin Strategy & Research compiled consumer  
 17  
 18  
 19  
 20

---

21       <sup>14</sup>See FTC Identity Theft Website: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

22       <sup>15</sup>The FTC defines identity theft as “a fraud committed or attempted using the identifying  
 23 information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes  
 24 “identifying information” as “any name or number that may be used, alone or in conjunction with  
 25 any other information, to identify a specific person,” including, among other things, “[n]ame, social  
 26 security number, date of birth, official State or government issued driver’s license or identification  
 27 number, alien registration number, government passport number, employer or taxpayer  
 28 identification number.” *Id.*

26       <sup>16</sup>See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can  
 27 You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), available at <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

28       <sup>17</sup>Brook, *What’s the Cost of a Data Breach in 2019*, *supra*.

28       <sup>18</sup>Norton By Symantec, 2013 Norton Report 8 (2013), available at  
[https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton\\_raportti.pdf](https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf).

1 complaints from the FTC and indicated that the median out-of-pocket cost to  
 2 consumers for identity theft was \$375.<sup>19</sup>

3 35. A person whose PII has been compromised may not see any signs of  
 4 identity theft for years. According to the GAO Report:

5 [L]aw enforcement officials told us that in some cases, stolen data  
 6 may be held for up to a year or more before being used to commit  
 7 identity theft. Further, once stolen data have been sold or posted on  
 8 the Web, fraudulent use of that information may continue for years.  
 9 As a result, studies that attempt to measure the harm resulting from  
 10 data breaches cannot necessarily rule out all future harm.

11 36. For example, in 2012, hackers gained access to LinkedIn's users'  
 12 passwords. However, it was not until May 2016, four years after the breach, that  
 13 hackers released the stolen email and password combinations.<sup>20</sup>

14 37. It is within this context that Plaintiff and thousands of other individuals  
 15 subjected to the Data Breach must now live with the knowledge that their PII and/or  
 16 PHI was disclosed to unauthorized persons, is likely forever in cyberspace and likely  
 17 available for sale on the dark web or black market.

18 ***Defendant's Business and Collection of Personal Information***

19 38. Defendant was founded in 2006 and began offering direct-to-consumer  
 20 genetic testing in November 2007 wherein customers, including Plaintiff and the Class  
 21 members, purchase Defendant's DNA test kits, Defendant's Ancestry Service, Health  
 22 + Ancestry Service, and/or 23andMe+ Membership, and provide Defendant with their  
 23 personal information and a saliva sample that is laboratory analyzed, using single  
 24 nucleotide polymorphism genotyping, to generate reports relating to the customer's  
 25 ancestry and genetic predispositions to health-related topics, including health reports  
 26 on genetic health risk, carrier status, wellness, and pharmacogenetics. Defendant also

---

27 <sup>19</sup>Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, available at  
 28 <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (citing the Javelin  
 report).

<sup>20</sup> See Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), available at  
<https://blog.linkedin.com/2016/05/18/protecting-our-members>.

1 offers an annual membership that contains everything in the health and ancestry service  
 2 plus access to ongoing genetic insights.

3       39. In the course of its business practices, Defendant collects and stores  
 4 customers' personal information in its system and networks, including electronically  
 5 and through its website and mobile applications.

6       40. Defendant's Privacy Policy,<sup>21</sup> which is incorporated by reference in its  
 7 Terms of Service,<sup>22</sup> acknowledges that it collects, stores, and transmits a substantial  
 8 amount of personal information from consumers, including:

- 9       □ **Individual-level Information:** information about a single individual,  
 10       such as their genotypes, diseases or other traits or characteristics.
- 11       □ **De-identified Information:** information that has been stripped of  
 12       identifying data, such as name and contact information, so that an  
 13       individual cannot reasonably be identified.
- 14       □ **Registration Information:** information you provide during account  
 15       registration or when purchasing the Services, such as a name, user ID,  
 16       password, date of birth, billing address, shipping address, payment  
 17       information (e.g., credit card), account authentication information, or  
 18       contact information (e.g., email, phone number).
- 19       □ **Genetic Information:** information regarding your genotype (e.g., the  
 20       As, Ts, Cs, and Gs at particular locations in your DNA). Genetic  
 21       Information includes the 23andMe genetic data and reports provided to  
 22       you as part of our Services.
- 23       □ **Sample Information:** information regarding any sample, such as a  
 24       saliva sample, that you submit for processing to be analyzed to provide  
 25       you with Genetic Information, laboratory values or other data provided  
 26       through our Services.

---

27  
 28<sup>21</sup> <https://www.23andme.com/legal/privacy/full-version/> (last updated October 4, 2023).

<sup>22</sup> <https://www.23andme.com/legal/terms-of-service/>

1           □ **Self-Reported Information:** information you provide to 23andMe  
 2           including your gender, disease conditions, health-related information,  
 3           traits, ethnicity, family history, or anything else you provide to us within  
 4           our Service(s).

5           □ **Biometric information:** certain Self-Reported Information you provide  
 6           to us or our service providers to verify your identity using biological  
 7           characteristics.

8           □ **User Content:** information, data, text, software, music, audio,  
 9           photographs, graphics, video, messages, or other materials, other than  
 10           Genetic Information and Self-Reported Information, generated by users  
 11           of 23andMe Services and transmitted, whether publicly or privately, to  
 12           or through 23andMe. For example, User Content includes comments  
 13           posted on our Blog or messages you send through our Services.

14           □ **Web-Behavior Information:** information on how you use our Services  
 15           or about the way your devices use our Services is collected through log  
 16           files, cookies, web beacons, and similar technologies (e.g., device  
 17           information, device identifiers, IP address, browser type, location,  
 18           domains, page views).

19           ***Defendant's Promises to Safeguard Customer PII***

20           41. Defendant represents and claims that: "We implement physical, technical,  
 21           and administrative measures aimed at preventing unauthorized access to or disclosure  
 22           of your Personal Information. Our team regularly reviews and improves our security  
 23           practices to help ensure the integrity of our systems and your Personal Information."<sup>23</sup>

24           42. Defendant's Terms of Service agreement incorporates by reference  
 25           Defendant's Privacy Policy.<sup>24</sup>

28           

---

23 <https://www.23andme.com/legal/privacy/full-version> (last updated October 4, 2023)

24 <https://www.23andme.com/legal/terms-of-service/>

## *The Data Breach*

2       43. On or about October 6, 2023, Defendant publicly announced via its  
3 website<sup>25</sup> that customer profile information shared through its DNA Relatives feature  
4 was compiled from individual 23andMe.com accounts, without account users'  
5 authorization, that contained the personally identifiable information ("PII") and/or  
6 protected health information ("PHI") of its customers (the "Data Breach").  
7 Defendant's website notice entitled "Addressing Data Security Concerns" further  
8 stated, "[w]e believe that the threat actor may have then, in violation of  
9 [Defendant's] Terms of Service, accessed 23andMe.com accounts without  
10 authorization and obtained information from certain accounts, including information  
11 about users' DNA Relatives profiles."

12       44. On or about October 11, 2023, Defendant sent Plaintiff and similarly  
13 situated Class members additional notifications via email related to the Data Breach,  
14 which similarly stated, “[w]e recently learned that certain profile information – which  
15 a customer creates and chooses to share with their genetic relatives in the DNA  
16 Relatives feature – was accessed from individual 23andMe.com accounts. This was  
17 done without the account users’ authorization.”

18        45. Defendant proclaimed its data security and safety in its Data Breach  
19 notifications which stated, “23andMe is committed to providing you with a safe and  
20 secure place where you can learn about your DNA knowing your privacy is protected;”  
21 and “[a]t 23andMe, we take security seriously. We exceed industry data protection  
22 standards and have achieved three different ISO certifications to demonstrate the  
23 strength of our security program. We actively and routinely monitor and audit our  
24 systems to ensure that your data is protected.”<sup>26</sup>

<sup>28</sup> <sup>25</sup> <https://blog.23andme.com/articles/addressing-data-security-concerns> (last accessed October 13, 2023)

26 *Id.*

1       46. Defendant's Data Breach notifications were misleading and inadequate  
 2 and did not provide any detail regarding when or for how long the Data Breach  
 3 occurred. Further, Defendant's Data Breach notices failed to indicate the scope of the  
 4 Data Breach or the specific information that was accessed, obtained from Defendant's  
 5 system without authorization and whether any of the PII and/or PHI accessed and/or  
 6 exfiltrated by the unauthorized person was recovered.

7       47. Defendant offered a limited number of recommendations for Plaintiff and  
 8 the Class members on how to protect against identity theft and fraud. These steps  
 9 included confirming they had a strong password, using multi-factor authentication  
 10 (MFA) on their 23andMe account, and reviewing their Privacy and Security Checkup  
 11 Page. Defendant did not offer Plaintiff and the Class members any identity monitoring  
 12 services or fraud insurance and failed to address the fact that victims of data breaches  
 13 and other unauthorized disclosures commonly face multiple years of ongoing identity  
 14 theft and/or fraud.

15       48. Plaintiff and the Class members' PII stolen in the Data Breach can be  
 16 misused on its own or can be combined with personal information from other sources  
 17 such as publicly available information, social media, etc. be used to commit further  
 18 identity theft and/or fraud. Plaintiff and the Class members suffer imminent and  
 19 continuing injury arising from the heightened risk of fraud and identity theft due to the  
 20 Data Breach, particularly because Plaintiff's and the Class members' personal  
 21 information stolen from Defendant in the Data Breach is already leaked and made  
 22 available for sale and/or purchased by criminals on the dark web.

23       49. Multiple sources, such as NBC News, have reported: "A database that has  
 24 been shared on dark web forums and viewed by NBC News has a list of 999,999 people  
 25 who allegedly have used the service. It includes their first and last name, sex, and  
 26 23andMe's evaluation of where their ancestors came from."<sup>27</sup>

27 <https://www.nbcnews.com/news/us-news/23andme-user-data-targeting-ashkenazi-jews-leaked-online-rcna119324>

1                   ***Defendant Knew or Should Have Known PII Are High Risk Targets***

2       50. Defendant knew or should have known that PII at issue here, like the  
 3 personal information of Plaintiff and the Class members, are high risk targets for  
 4 identity thieves.

5       51. The Identity Theft Resource Center reported that the business sector had  
 6 the largest number of breaches in 2018. According to the ITRC this sector suffered 571  
 7 data breaches exposing at least 415,233,143 million records in 2018.<sup>28</sup> Further, the  
 8 ITRC identified “hacking” as the most common form of data breach in 2018,  
 9 accounting for 39% of data breaches.

10      52. Prior to the breach there were many reports of high-profile data breaches  
 11 that should have put a company like Defendant on high alert and forced it to closely  
 12 examine its own security procedures, as well as those of third parties with which it did  
 13 business and gave access to its subscriber PII. Notable breaches included Capital One,  
 14 which announced that in March 2019 a hacker had gained access to 100 million U.S.  
 15 customer accounts and credit card applications. Similarly, in December 2018, Marriott  
 16 International announced a data breach that affected up to 500 million individuals. The  
 17 data breach allowed hackers to access customer names, physical addresses, phone  
 18 numbers, email addresses, passport numbers, dates of birth, gender, loyalty program  
 19 account information, and payment card information.<sup>29</sup>

20      53. As such, Defendant was aware that PII is at high risk of theft, and  
 21 consequently should have but did not take appropriate and standard measures to protect  
 22 Plaintiff’s and Class members’ PII and/or PHI against data breaches and unauthorized  
 23 disclosures that Defendant should have anticipated and guarded against.

24  
 25  
 26                   <sup>28</sup> Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, available at  
 27 [https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC\\_2018-End-of-Year-Aftermath\\_FINAL\\_V2\\_combinedWEB.pdf](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf).

27                   <sup>29</sup> See <https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach#:~:text=Marriott%20International%20says%20that%20a,up%20to%20500%20million%20people.&text=The%20hotel%20chain%20says%20the,10%2C%202018%20could%20be%20affected>

## CLASS DEFINITION AND ALLEGATIONS

54. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks to represent and intend to certify a class defined as:

*All individuals whose personal information and/or PII was compromised in the Data Breach (the “Class”).*

55. In addition, Plaintiff seeks to represent and intends to certify a sub-class defined as:

*All California citizens whose personal information and/or PII was compromised in the Data breach (the “California Sub-Class”).*

56. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

57. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

58. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, upon information and belief the Class is so numerous that joinder of all members is impractical.

59. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

1       60. There is a well-defined community of interest in the common questions of  
2 law and fact affecting Class members. The questions of law and fact common to Class  
3 members predominate over questions affecting only individual Class members, and  
4 include without limitation:

5               (a) Whether Defendant had a duty to implement and maintain  
6 reasonable security procedures and practices appropriate to the  
7 nature of the PII it collected from Plaintiff and Class members;  
8               (b) Whether Defendant breached its duty to protect the PII of Plaintiff  
9 and Class members; and  
10               (c) Whether Plaintiff and Class members are entitled to damages and  
11 other equitable relief.

12       61. Plaintiff will fairly and adequately protect the interests of the Class  
13 members. Plaintiff is an adequate representative of the Class in that they has no  
14 interests adverse to or that conflicts with the Class they seek to represent. Plaintiff has  
15 retained counsel with substantial experience and success in the prosecution of complex  
16 consumer protection class actions of this nature.

17       62. A class action is superior to any other available method for the fair and  
18 efficient adjudication of this controversy since individual joinder of all Class members  
19 is impractical. Furthermore, the expenses and burden of individual litigation would  
20 make it difficult or impossible for the individual members of the Class to redress the  
21 wrongs done to them, especially given that the damages or injuries suffered by each  
22 individual member of the Class are outweighed by the costs of suit. Even if the Class  
23 members could afford individualized litigation, the cost to the court system would be  
24 substantial and individual actions would also present the potential for inconsistent or  
25 contradictory judgments. By contrast, a class action presents fewer management  
26 difficulties and provides the benefits of single adjudication and comprehensive  
27 supervision by a single court.

1       63.   Defendant has acted or refused to act on grounds generally applicable to  
2 the entire Class, thereby making it appropriate for this Court to grant final injunctive,  
3 including public injunctive relief, and declaratory relief with respect to the Class as a  
4 whole.

## **CAUSES OF ACTION**

## **FIRST CAUSE OF ACTION**

## **Violation of the California Consumer Privacy Act of 2018 (“CCPA”) Cal. Civ. Code §§ 1798.100, *et seq.***

8       64. Plaintiff realleges and incorporates by reference all preceding paragraphs  
9 as if fully set forth herein.

10       65. As more personal information about consumers is collected by businesses,  
11 consumers' ability to properly protect and safeguard their privacy has decreased.  
12 Consumers entrust businesses with their personal information on the understanding that  
13 businesses will adequately protect it from unauthorized access. The California  
14 Legislature explained: "The unauthorized disclosure of personal information and the  
15 loss of privacy can have devastating effects for individuals, ranging from financial fraud,  
16 identity theft, and unnecessary costs to personal time and finances, to destruction of  
17 property, harassment, reputational damage, emotional stress, and even potential  
18 physical harm."<sup>30</sup>

19       66. As a result, in 2018, the California Legislature passed the CCPA, giving  
20 consumers broad protections and rights intended to safeguard their personal  
21 information. Among other things, the CCPA imposes an affirmative duty on businesses  
22 that maintain personal information about California residents to implement and  
23 maintain reasonable security procedures and practices that are appropriate to the nature  
24 of the information collected. Defendant failed to implement such procedures which  
25 resulted in the Data Breach.

<sup>28</sup> <sup>30</sup>California Consumer Privacy Act (CCPA) Compliance, <https://buyergenomics.com/ccpa-compliance/>.

1       67. It also requires “[a] business that discloses personal information about a  
 2 California resident pursuant to a contract with a nonaffiliated third party . . . [to] require  
 3 by contract that the third party implement and maintain reasonable security procedures  
 4 and practices appropriate to the nature of the information, to protect the personal  
 5 information from unauthorized access, destruction, use, modification, or disclosure.”  
 6 1798.81.5(c).

7       68. Section 1798.150(a)(1) of the CCPA provides: “Any consumer whose  
 8 nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject  
 9 to an unauthorized access and exfiltration, theft, or disclosure as a result of the  
 10 business’ violation of the duty to implement and maintain reasonable security  
 11 procedures and practices appropriate to the nature of the information to protect the  
 12 personal information may institute a civil action for” statutory or actual damages,  
 13 injunctive or declaratory relief, and any other relief the court deems proper.

14       69. Plaintiff and Class members are “consumer[s]” as defined by Civ. Code  
 15 § 1798.140(g) because they are “natural person[s] who [are] California resident[s], as  
 16 defined in Section 17014 of Title 18 of the California Code of Regulations, as that  
 17 section read on September 1, 2017.

18       70. Defendant is a “business” as defined by Civ. Code § 1798.140(c) because  
 19 Defendant:

20               (a) is a “sole proprietorship, partnership, limited liability company,  
 21 corporation, association, or other legal entity that is organized or operated for the  
 22 profit or financial benefit of its shareholders or other owners”;

23               (b) “collects consumers’ personal information, or on the behalf of  
 24 which is collected and that alone, or jointly with others, determines the purposes  
 25 and means of the processing of consumers’ personal information”;

26               (c) does business in California; and

27               (d) has annual gross revenues in excess of \$25 million; annually  
 28 buys, receives for the business’ commercial purposes, sells or shares for

1 commercial purposes, alone or in combination, the personal information of 50,000  
2 or more consumers, households, or devices; or derives 50 percent or more of its  
3 annual revenues from selling consumers' personal information.

4 71. The PII taken in the Data Breach is "personal information" as defined by  
5 Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and Class members'  
6 personal information, which upon information and belief includes name, sex, date of  
7 birth, DNA and genetic ancestry results, profile photos, geographical information, and  
8 other sensitive personal information.

9 72. Plaintiff's PII was subject to unauthorized access, exfiltration, or  
10 disclosure because their PII was wrongfully disclosed and accessed by unauthorized  
11 third parties.

12 73. The Data Breach occurred as a result of Defendant's failure to implement  
13 and maintain reasonable security procedures and practices appropriate to the nature of  
14 the information to protect Plaintiff's and Class members' PII, including to ensure that  
15 it had sufficient security protocols in place to protect the PII to which Defendant  
16 maintained and/or gave third parties access to. Defendant failed to implement  
17 reasonable security procedures to prevent unauthorized access and disclosure of  
18 Plaintiff's and Class members' PII as a result of this Data Breach.

19 74. On or around October 13, 2023, Plaintiff sent Defendant written notice of  
20 its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Exhibit A. In  
21 the event Defendant does not, or is unable to, cure the violation within 30 days, Plaintiff  
22 will amend the operative complaint to pursue statutory damages as permitted by Civil  
23 Code § 1798.150(a)(1)(A).

24 75. As a result of Defendant's failure to implement and maintain reasonable  
25 security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual  
26 damages, injunctive relief, including public injunctive relief, and declaratory relief, and  
27 any other relief as deemed appropriate by the Court.

**SECOND CAUSE OF ACTION**  
**Violation of the California Unfair Competition Law (“UCL”)**  
**Cal. Bus. & Prof. Code §§ 17200, *et seq.***

3       76. Plaintiff re-alleges and incorporates by reference all proceeding  
4 paragraphs as if fully set forth herein.

5       77. The UCL prohibits any “unlawful,” “fraudulent” or “unfair” business act  
6 or practice and any false or misleading advertising, as those terms are defined by the  
7 UCL and relevant case law. By virtue of the above-described wrongful actions,  
8 inaction, omissions, and want of ordinary care that directly and proximately caused the  
9 Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within  
10 the meaning, and in violation of, the UCL.

11       78. In the course of conducting its business, Defendant committed “unlawful”  
12 business practices by, *inter alia*, knowingly failing to design, adopt, implement,  
13 control, direct, oversee, manage, monitor and audit appropriate data security processes,  
14 controls, policies, procedures, protocols, and software and hardware systems to  
15 safeguard and protect Plaintiff’s and Class members’ PII, and by violating the statutory  
16 and common law alleged herein, including, *inter alia*, California Consumer Privacy  
17 Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq.*) and Article I, Section 1 of the  
18 California Constitution (California’s constitutional right to privacy), Customer  
19 Records Act (“CRA”) (Cal. Civ. Code §§ 1798.80, *et seq.*, and Civil Code § 1798.81.5.  
20 Plaintiff and Class members reserve the right to allege other violations of law by  
21 Defendant constituting other unlawful business acts or practices. Defendant’s above-  
22 described wrongful actions, inaction, omissions, and want of ordinary care are ongoing  
23 and continue to this date.

24       79. Defendant also violated the UCL’s unlawful prong by breaching  
25 contractual obligations created by its Privacy Policies and by knowingly and willfully  
26 or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code §  
27 22576, which prohibits a commercial website operator from “knowingly and willfully”  
28 or “negligently and materially” failing to comply with the provisions of its posted

1 privacy policy. Plaintiff and Class members suffered injury in fact and lost money or  
2 property as a result of Defendant's violations of its Terms of Service and/or Privacy  
3 Policy.

4       80. Defendant's above-described wrongful actions, inaction, omissions, want  
5 of ordinary care, misrepresentations, practices, and non-disclosures also constitute  
6 "unfair" business acts and practices in violation of the UCL in that Defendant's  
7 wrongful conduct is substantially injurious to consumers, offends legislatively-  
8 declared public policy, and is immoral, unethical, oppressive, and unscrupulous.  
9 Defendant's practices are also contrary to legislatively declared and public policies that  
10 seek to protect PII and ensure that entities who solicit or are entrusted with personal  
11 data utilize appropriate security measures, as reflected by laws such as the CCPA,  
12 Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45).  
13 The gravity of Defendant's wrongful conduct outweighs any alleged benefits  
14 attributable to such conduct. There were reasonably available alternatives to further  
15 Defendant's legitimate business interests other than engaging in the above-described  
16 wrongful conduct.

17       81. Plaintiff and Class members suffered injury in fact and lost money or  
18 property as a result of Defendant's violations of its Privacy Policy and statutory and  
19 common law in that a portion of the money Plaintiff and Class members paid, or that  
20 Defendant received, for Defendant's products and services went to fulfill the  
21 contractual obligations set forth in its Privacy Policy, including maintaining the  
22 security of their PII, and Defendant's legal obligations, and Defendant failed to fulfill  
23 those obligations.

24       82. The UCL also prohibits any "fraudulent business act or practice." Defendant's  
25 above-described claims, nondisclosures and misleading statements were  
26 false, misleading, and likely to deceive the consuming public in violation of the UCL.

27       83. As a direct and proximate result of Defendant's above-described wrongful  
28 actions, inaction, omissions, and want of ordinary care that directly and proximately

1 caused the Data Breach and its violations of the UCL, Plaintiff and Class members  
2 have suffered injury in fact and lost money or property as a result of Defendant's unfair  
3 and deceptive conduct. Such injury includes paying for a certain level of security for  
4 their PII but receiving a lower level, paying more for Defendant's products and services  
5 than they otherwise would have had they known Defendant was not providing the  
6 reasonable security represented in its Privacy Policy and as in conformance with its  
7 legal obligations. Had Plaintiff and Class members known about Defendant's  
8 substandard data security practices they would not have purchased Defendant's  
9 products or services or would have paid less for them. Defendant's security practices  
10 have economic value in that reasonable security practices reduce the risk of theft of  
11 customer's PII.

12 84. Plaintiff and Class members have also suffered (and will continue to  
13 suffer) economic damages and other injury and actual harm in the form of, *inter alia*,  
14 (i) an imminent, immediate and the continuing heightened increased risk of identity  
15 theft and identity fraud – risks justifying expenditures for protective and remedial  
16 services for which they are entitled to compensation, (ii) invasion of privacy,  
17 (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA,  
18 (v) deprivation of the value of their PII for which there is a well-established national  
19 and international market, and/or (vi) the financial and temporal cost of monitoring their  
20 credit, monitoring accounts, and mitigating damages.

21 85. Unless restrained and enjoined, Defendant will continue to engage in the  
22 above-described wrongful conduct and more data breaches will occur. Plaintiff,  
23 therefore, on behalf of himself, the Class members, and the general public, also seeks  
24 restitution and an injunction, including public injunctive relief prohibiting Defendant  
25 from continuing such wrongful conduct, and requiring Defendant to modify its  
26 corporate culture and design, adopt, implement, control, direct, oversee, manage,  
27 monitor and audit appropriate data security processes, controls, policies, procedures  
28 protocols, and software and hardware systems to safeguard and protect the PII entrusted

1 to it, as well as all other relief the Court deems appropriate, consistent with Bus. &  
 2 Prof. Code § 17203.

3 **THIRD CAUSE OF ACTION**

4 **Breach of Contract**

5 86. Plaintiff re-alleges and incorporates by reference all proceeding  
 6 paragraphs as if fully set forth herein.

7 87. Plaintiff and Class members entered into express or implied contracts with  
 8 Defendant as set forth in its Terms of Service that included Defendant's promise to  
 9 protect nonpublic personal information given to Defendant or that Defendant gathered  
 10 on its own, from disclosure, as set forth in Defendant's Privacy Policy, which was  
 11 posted on its website, and expressly incorporated into Defendant's Terms of Service.

12 88. Plaintiff and Class members performed their obligations under the  
 13 contracts when they provided their PII to Defendant, or Defendant collected and  
 14 maintained their PII; however, Plaintiff and the Class members did not receive the full  
 15 benefit of the bargain from Defendant.

16 89. Defendant breached its contractual obligation to protect the PII Defendant  
 17 gathered when the information was exposed to, accessed, and exfiltrated by  
 18 unauthorized third parties as part of the Data Breach.

19 90. As a direct and proximate result of the Data Breach, Plaintiff and Class  
 20 members have been harmed and have suffered, and will continue to suffer, damages  
 21 and injuries.

22 **FOURTH CAUSE OF ACTION**

23 **Negligence**

24 91. Plaintiff re-alleges and incorporates by reference all proceeding  
 25 paragraphs as if fully set forth herein.

26 92. Defendant owed various duties to Plaintiff and the Class, including  
 27 pursuant to the CCPA, as alleged in detail above. Defendant owed duties to Plaintiff  
 28 and the Class with regard to their manner of collection, transmission, sharing, and

1 maintenance of Plaintiff's and the Class members' personal data, including PII, and  
 2 were required to maintain reasonable security procedures and practices to safeguard  
 3 Plaintiff's and the Class members personal information. Defendant further owed  
 4 Plaintiff and the Class the duty to promptly notify them of the scope and nature of the  
 5 Data Breach.

6 93. Defendant breached its respective duties by engaging in the conduct and  
 7 omissions alleged above and in violation of the CCPA and UCL, as well as its Privacy  
 8 Policy as alleged above.

9 94. Defendant is both the actual and legal cause of Plaintiff's and the Class  
 10 members' damages.

11 95. Plaintiff believes and thereon alleges that as a proximate result of  
 12 Defendant's negligence, Plaintiff and the Class have suffered actual damages, invasion  
 13 and loss of privacy, and emotional distress as described herein and above.

14 96. Due to the egregious violations alleged herein, Plaintiff asserts that  
 15 Defendant breached its duties in an oppressive, malicious, despicable, gross, and  
 16 wantonly negligent manner. Defendant's conscious disregard for Plaintiff's privacy  
 17 rights entitles Plaintiff and the Class to recover punitive damages.

18 **PRAYER FOR RELIEF**

19 **WHEREFORE**, Plaintiff, on behalf of himself and all members of the Class  
 20 respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be  
 21 designated a representative of the Class, and (iii) Plaintiff's counsel be appointed as  
 22 counsel for the Class. Plaintiff, on behalf of himself and members of the Class further  
 23 requests that upon final trial or hearing, judgment be awarded against Defendant for:

24 (i) actual and punitive damages to be determined by the trier of fact;  
 25 (ii) equitable relief, including restitution;  
 26 (iii) pre- and post-judgment interest at the highest legal rates applicable;  
 27 (iv) appropriate injunctive relief;

1 (v) attorneys' fees and litigation expenses under Code of Civil  
2 Procedure § 1021.5 and other applicable law;  
3 (vi) costs of suit; and  
4 (vii) such other and further relief the Court deems just and proper.

5 **DEMAND FOR JURY TRIAL**

6 Plaintiff hereby demands a jury trial on all issues so triable.

7  
8 Dated: October 13, 2023

Respectfully submitted,

9 **KAZEROUNI LAW GROUP, APC**

10 By: /s/ Abbas Kazerounian  
11 Abbas Kazerounian, Esq.  
12 Mona Amini, Esq.  
13 245 Fischer Avenue, Unit D1  
14 Costa Mesa, California 92626  
Telephone: (800) 400-6808  
Facsimile: (800) 520-5523

15 *Attorneys for Plaintiff*



# EXHIBIT A



245 Fischer Avenue, Unit D1  
Costa Mesa, California 92626  
Telephone: (800) 400-6808  
Facsimile: (800) 520-5523  
[www.kazlg.com](http://www.kazlg.com)

October 13, 2023

**VIA CERTIFIED MAIL**

23ANDME, INC.  
349 OYSTER POINT BLVD  
SOUTH SAN FRANCISCO CA 94080

**Re: Haris Mirza v. 23andMe, Inc.**

*Notice of Violations of the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.*

To Whom It May Concern:

This office represents Plaintiff Haris Mirza (“Plaintiff”) and all other similarly situated consumers in a putative class action against 23andMe, Inc. (“Defendant”) arising out of, *inter alia*, Defendant’s failure to provide reasonable security for Plaintiff’s and the proposed Class members’ personal information, which resulted in the unauthorized access, theft, or disclosure of this data (the “Data Breach”). To our knowledge, Defendant has announced the Data Breach via its blog/website beginning on or around October 6, 2023, and via e-mail to Plaintiff and the Class members on or around October 11, 2023.

Plaintiff’s claims, including the facts and circumstances surrounding these claims are detailed in Plaintiff’s Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant’s conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of Plaintiff’s claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiff with an express written statement within thirty (30) days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiff and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

*s/ Abbas Kazerounian*

Abbas Kazerounian, Esq.  
KAZEROUNI LAW GROUP, APC  
Direct Line: (800) 400-6808, Ext. 2  
E-mail: [ak@kazlg.com](mailto:ak@kazlg.com)

[Enclosure]